Axidian

WHITE PAPER

Axidian Privilege

Managing Privileged Access to Corporate IT Systems

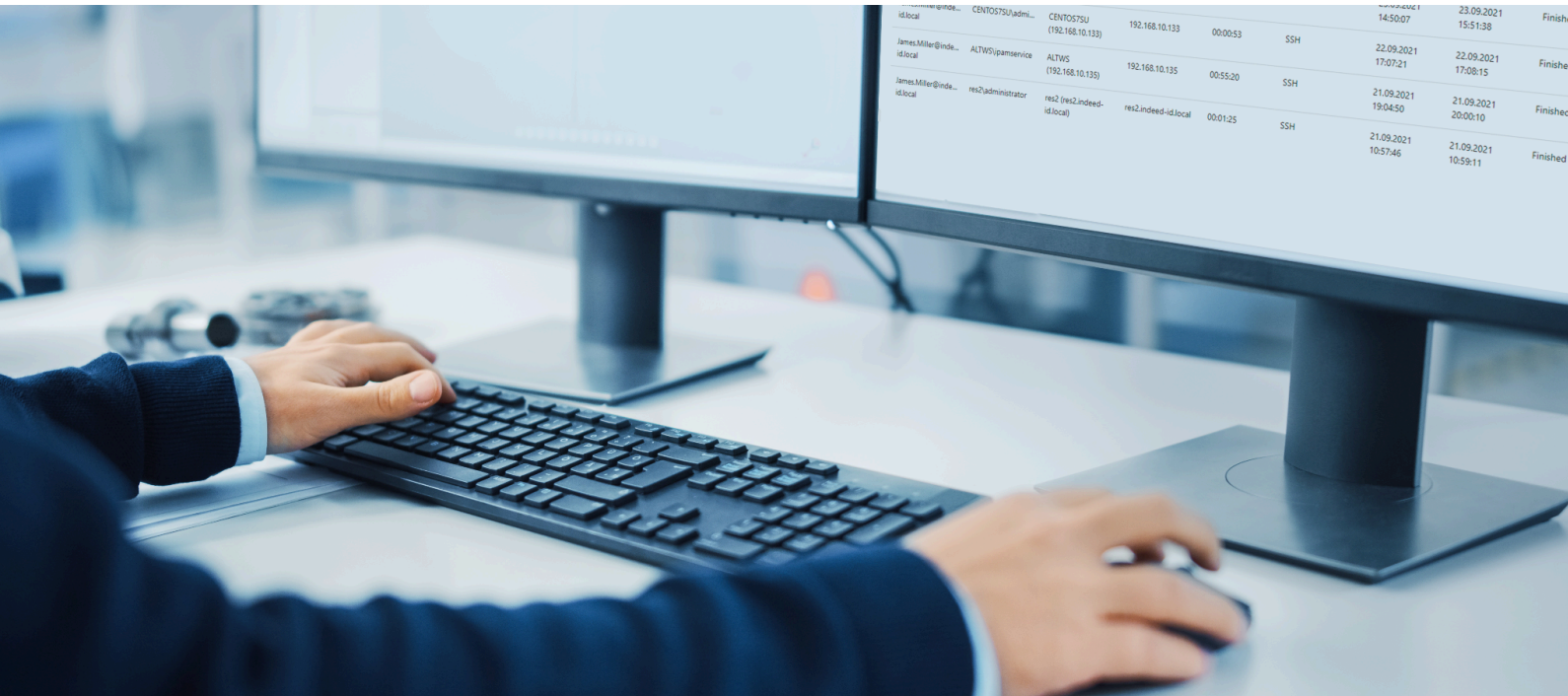

Table of contents

Privileged access – a potential security threat

Continuous growth, sophistication, and upgrades of IT infrastructure make privileged access management a top priority for ensuring cybersecurity. The increasing number of information systems and the variety of access scenarios can make this task rather challenging. A malicious user with access to an administrator account can cause your company way more serious damage compared to regular employees with compromised credentials. Administrator accounts can be used to disable the security system, stop the operation of information systems, and gain access to confidential information. Ensuring privileged access security is a sophisticated task; it cannot be achieved by relying exclusively on standard approaches to the protection of credentials and requires specialized solutions.

Privileged users

Privileges may be assigned to various categories of in-house and external personnel, which means that all these users can gain access to essential information and critical hardware and software functions.

Information system administrators

Each device and application or system software have their own administrator accounts. The fact that administrators should have privileged access rights is self-evident. Such employees may include:

- Active Directory administrators
- Network equipment administrators
- Database administrators
- Server administrators (Windows, Unix/Linux)
- VDI administrators

Business users

Although business users do not have administrative rights, they may still have wide-ranging privileges in specific information systems. For example, they may be able to transfer money, manage production processes, and gain access to data marked as a trade secret.

Contractors and partners

Contractors' employees are normally responsible for maintenance of specialized software and hardware. They may work for a vendor or integrator. These users usually have remote access to corporate infrastructure, which can make the oversight of their operations rather challenging.

Service accounts

Service accounts are needed for process automation. They are utilized to run various services, daemons, scripts, and other software. You can easily forget about such accounts since employees don't use them explicitly every day. And this leads to additional challenges and risks.

Privileged access management

If you want to manage and protect your corporate privileged access effectively, make sure that you do the following:

- Centrally manage access of your employees to controlled resources.
- Prevent uncontrolled use of privileged accounts, i.e., discover them and take them under control. Keep the passwords secret, perform regular checks, and change passwords to random values.
- Reduce the number of privileged accounts required to manage your corporate information systems. Keep an access log containing records of all attempts to use privileged accounts (it must clearly state which employee gained access to which account and when).
- Enable multi-factor authentication for access to privileged accounts.
- Use special mechanisms for investigating incidents and restoring the sequence of events, monitor privileged user activity, and assess the work performed under privileged accounts.

Axidian Privilege (PAM) is an access management system for corporate infrastructure with privileged accounts. Below you will learn how Axidian Privilege can help you solve these problems.

Centralized access management

Axidian Privilege keeps records of information about all privileged accounts and related permissions. Permissions are the key tool used for granting privileged access in Axidian Privilege. Permissions are used to define the following access parameters:

- Who – which users or user groups have access.
- Where – which servers, hardware, and applications users can work with.
- Access rights – which user account will be used for connection and whether the user is authorized to view or change passwords or SSH keys to accounts.
- Terms – access period and schedule, the types of protocols to be used, and resources that will be available to users depending on the network location of connection points.

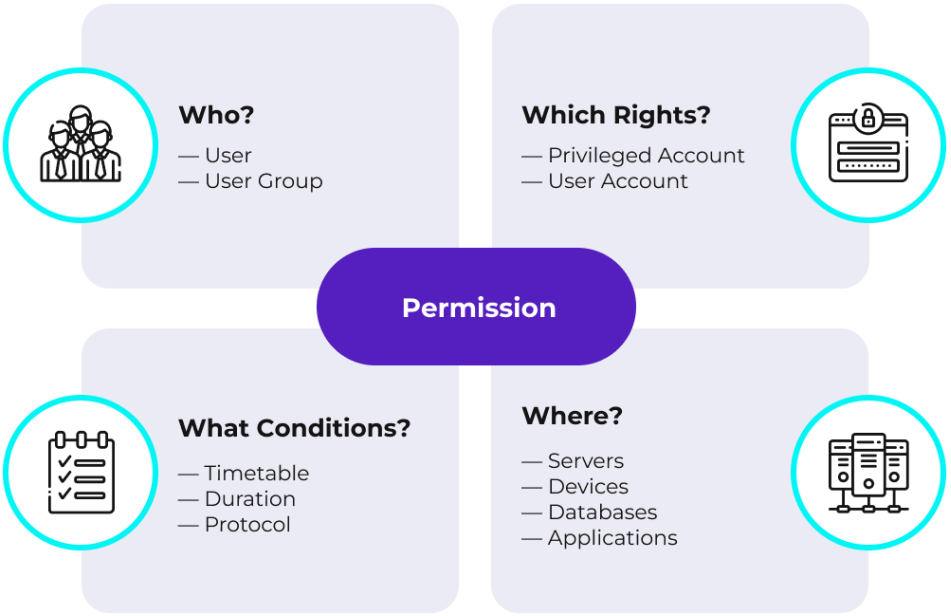

Figure 1. Access permission settings

Permissions are centrally assigned by an administrator in the Axidian Privilege management console. Permissions may be temporarily suspended or revoked if access is no longer required. Axidian Privilege supports integration with Service/Help Desk systems. Thanks to this option, your personnel may continue using the same familiar system to request access approvals, while permissions will be automatically granted and revoked via Axidian Privilege as part of this workflow. Axidian Privilege offers two interaction paths for this purpose: a command-line utility and a web application programming interface (API).

In addition to permissions, the system includes one more access management tool – Axidian Privilege policies. Policies are used to define general access parameters such as:

- Permitted and forbidden commands in SSH sessions.
- Whether commands to assign root privileges are allowed.
- Whether the PAM administrator's approval is required for new privileged sessions.
- PC local resources available on a remote resource (disks, clipboard, etc.).
- Whether a privileged account password and SSH key should be reset after the end of a session.
- Exclusive mode for privileged accounts (one user account can be used to initiate one session only).
- The maximum duration of a privileged session.
- Whether a user is authorized to view the privileged account password.
- Whether a privileged account password and SSH key should be reset after they are shown to a user.

- Whether users are required to provide a reason to view the password and SSH key.
- Whether the PAM administrator's approval is required to view the password and SSH key to an account.
- Whether a video recording, screenshots, or text logs of the session should be saved.
- Whether shadow copying is required for all files transferred during the sessions.
- Etc.

Controlled use of privileged accounts

Axidian Privilege relies on four mechanisms to exercise control over the use of privileged accounts:

- Discovery of privileged accounts
- Storage of credentials
- Rotation of passwords and SSH keys
- Secure use of credentials

User account discovery

Axidian Privilege incorporates Account Discovery, a tool designed for running regular searches for new accounts across all connected resources and domains. You can customize the search frequency and set different frequency for specific groups of resources. Upon discovery of a new account that is not yet registered in the PAM system, relevant information is added to the shared repository. In addition, the relevant event is recorded in the log, and the administrator may opt to get email notifications about such events, so that they can make a prompt decision regarding the use of the new account. Axidian Privilege supports account searches across the following types of resources:

- Workstations and servers running Windows[1]
- *nix systems
- DBMS (MS SQL, MySQL, PostgreSQL, Oracle)
- Active Directory
- Cisco IOS
- Inspur BMC

Credential storage

Axidian Privilege is used as a centralized repository for privileged credentials that can only be accessed with a valid permission. Without appropriate permissions, even the PAM administrator will not be able to view passwords and SSH keys.

In addition to storage, Axidian Privilege performs regular checks of passwords and SSH

[1] The current version permits local user account searches, and future versions will feature searches for service accounts used to run services and scheduled tasks.

keys to make sure that all credentials in the system are up to date. In the event of a mismatch, such passwords and SSH keys may be reset and the relevant notification may be sent to the PAM administrator.

You can also opt to automatically discover and delete SSH keys that are not managed by PAM on resources.

Password and SSH key rotation

Axidian Privilege changes passwords and SSH keys to random values according to a pre-set schedule in order to maintain their security. You can customize the complexity of generated passwords in line with your company's security policies.

All previous passwords and SSH keys are also stored in the PAM password history. This way, you can roll back a password or key to any desired point in the past. This function will be essential if you need to restore a target resource using a backup copy, and you need the credentials applicable at the time of creation of the backup copy.

Secure use of privileged credentials

With Axidian Privilege, your company can choose to avoid explicit use of privileged credentials by your employees. Administrators in charge of servers, network equipment, Active Directory, and application systems no longer need to have administrative credentials – PAM can do this job on their behalf. Your staff member can connect to PAM via their user account, and a new session will be opened on the target resource under a user account with appropriate rights. This way, you can prevent uncontrolled use of privileged accounts and make sure that your personnel can no longer keep their credentials in an insecure place (in a file stored on the desktop or network drive, on stickers, etc.) or intentionally disclose passwords to third parties.

With Indeed PAM, you can also enable exclusive mode for your most important privileged accounts. In the exclusive mode, one privileged account can be used to launch one session only. This can help you avoid any problems that may arise if simultaneous changes are made in the managed systems.

Single Sign-On

With Axidian Privilege, new sessions can be launched with transparent transfer of credentials to the target resource, and this option is available not only for classic remote access protocols such as RDP, SSH, or Telnet. The system includes a specialized SSO agent (Single Sign-On agent) that can automatically add credentials in web and desktop applications. Thanks to the SSO agent, Axidian Privilege can ensure transparent access to network hardware administration web interfaces, fat DBMS clients, and other apps.

Application-to-Application Password Management

Your employees are not the only ones who can have user accounts with higher access rights. Many automation tools (apps, scripts, etc.) rely on service accounts to perform their functions. Axidian Privilege offers an API for obtaining up-to-date service credentials to avoid storing passwords in scripts and configuration files. All operations related to obtaining new passwords will be recorded in the PAM log, and all passwords will be changed to random values after a specified period of time.

Reduced number of privileged accounts

The Account Discovery tool can help you promptly identify the accounts that your administrators and information security staff may have forgotten about (for example, temporary accounts that have not been deleted or disabled in due time). Thanks to this regular “stock taking”, you can keep your pool of privileged accounts up to date and avoid redundancy. This, in turn, can help you reduce the potential attack surface and enhance cybersecurity in your company.

With PAM, you may choose not to set up personal accounts for administrators altogether, minimizing the number of privileged accounts in your company. Axidian Privilege captures all events that have to do with access to managed resources and keeps logs of:

- Employees who gained access to a given resource.
- Resources to which access was granted.
- User accounts used for gaining access to resources.
- Session date and time.
- Session duration.
- Utilized access protocol.

This way, even if anonymized accounts are used for connections to resources (administrator, root, etc.), PAM will retain the information about the employees who performed specific operations.

Multi-factor authentication

When it comes to privileged accounts, it's crucial to have robust authentication methods in place to make sure that only authorized users can access company resources and that they cannot deny their actions. Axidian Privilege out-of-the-box solution supports two-factor user authentication that includes a password and TOTP (Time-Based One-Time Password). In this case, users are expected to use an app installed on their smartphone to generate a one-time password. Axidian Privilege also supports two-factor authentication that includes a password and OTP sent by email. You can also opt to enable or disable two-factor authentication for all users or for each user individually.

If your company relies on standard Windows tools for user authentication, including smart cards and digital certificates, you may continue to use this authentication method for access via RDP.

The platform supports authentication of PAM users and administrators via AD, FreeIPA, or RADIUS server using the challenge-response mechanism. This enables integration with multi-factor authentication systems, such as Axidian Access. Axidian Access supports the following as a second factor: one-time passwords sent by email or SMS or generated in software and hardware generators, push authentication with access verification in mobile app, and one-time passwords with verification via Telegram. The following authentication protocols are supported for RADIUS: PAP, CHAP, and MS-CHAPv2.

Incident investigation

Privileged sessions can potentially cause disruptions in the standard operation of information systems or result in unwanted behavior. With works outsourced to contractors, you cannot always be sure that they have been duly performed to the full extent. In this case, it is essential to be able to identify the exact modifications made in the system operation, as well as the authors of these changes.

Axidian Privilege can capture user activity in the following formats:

- Video records showing the entire screen. You can customize video parameters such as image quality, resolution, and frame rate.
- Screenshots taken at regular intervals. This feature can be useful if you want to save disk space and record non-critical sessions.
- Session text logs. For SSH sessions, all user input/output is recorded; for RDP sessions, initiated processes, the headers of active windows, and user input are captured.

PAM administrators have the option to view sessions both in real time and after expiry. The administrator who monitors an active session can terminate it in the event of suspicious behavior.

All session materials (videos, screenshots, and text logs) can be downloaded for review and analysis in third-party solutions.

Axidian Privilege

Axidian Privilege composition

Figure 2. Axidian Privilege structure

Axidian Privilege includes the following logical and functional modules.

Policies and permissions

Policies and permissions are used to define the following privileged access parameters:

- Persons who are granted access to resources.
- User accounts to which access is granted.
- Resources (servers and hardware) to which access is granted.
- Timeframe (permanent/temporary access, access during business hours, or at any time).
- Type of session records (video records and text logs, text only, screenshots, etc.).
- Local resources (clipboard, disks, smart cards, etc.) that will be available to the user during the remote session.
- Whether a user is authorized to view the privileged account password.
- Etc.

Centralized policies can help you reduce the cost of system administration and make

the access parameters and rights transparent to information security professionals and auditors. For more information about policies and permissions, please see the Centralized access management section.

Credentials

The credentials (usernames, passwords, and SSH keys) required for access to resources are stored in a vault that can only be accessed by the Axidian Privilege server. Strong encryption algorithms are used to encrypt the data for storage and transmission from/to the server. The access to the vault is restricted and reserved exclusively for the PAM server. This is made possible thanks to a special procedure, whereby the database server is hardened.

Users

PAM users are employees who are assigned privileged access rights via the PAM system. Axidian Privilege uses Active Directory or FreeIPA as a user directory. User accounts are utilized for gaining access to the user console, access server, SSH Proxy, RDP Proxy, and management console.

Resources

A resource in Axidian Privilege is an object to which access is granted. In most cases, this means Windows and Linux servers. A specific application can also be a resource, for example, an app designed for managing DBMS or a web-based router configurator.

Organizational structure

You can assign different control rights to administrators in charge of specific departments and branches. The solution enables grouping of resources: you can create a separate resource container for every branch and assign the rights to control this container to a given PAM administrator. You can use the privileges in role settings to customize the administrative rights. The administrator will be able to view and grant permissions, view sessions, manage accounts and perform other functions, but only on resources added to the corresponding container.

Session log

All privileged sessions are recorded and saved in the Axidian Privilege archive. All records in the archive are encrypted and can only be accessed by users with appropriate PAM permissions. Sessions can be recorded in the following formats:

- Text logs are kept at all times and include the following data:
    - All input and output in the console for SSH connections.
    - All processes launched, windows opened, and keyboard input for RDP connections.
- Video records are available for both RDP and SSH connections. Video records

are optional and can be enabled in the policies by the PAM administrator. Video quality can be adjusted; you may set independent values for different user accounts. For example, you may record domain administrator sessions with maximum quality and operator sessions with compression.

- Screenshots are also available for both RDP and SSH connections. Screenshots are optional and can be enabled in the policies by the PAM administrator. Screenshot frequency and quality can be customized in the policies.

The PAM administrator can monitor active sessions in real time and terminate the session if needed.

For easy integration with SIEM tools and timely response to incidents, text logs of sessions may be sent via syslog to a third-party server. Supported log formats: LEEF, CEF. You can also pre-filter logs prior to sending.

Roles

The roles assigned to users determine their permissions in the Axidian Privilege management console. Three roles are available by default:

- Administrator − full access to all PAM functions and settings.
- Operator − authority to assign and revoke permissions.
- Inspector − read-only access.

You can change the privileges assigned for each role and adapt them to your company's needs. To set a more nuanced division of authorities, you can create your own roles.

Event log

Events can be logged in the Event Log or in a database both locally and on a dedicated Axidian Privilege server. Any activity of PAM administrators and users is regarded as events. All changes in the system parameters will be logged, as well as user information and credentials for all connections to target resources.

For easy integration with SIEM tools and timely response to incidents, events may be sent via syslog to a third-party log server. Supported log formats: LEEF, CEF.

Access server

The access server relies on a centralized privileged access model. First, a user is connected to the access server to complete an access rights check and one- or two-factor authentication, and then a new session on the target resource is launched.

The access server is powered by Microsoft RDS (Remote Desktop Services) server with pre-installed Axidian Privilege components. Upon connection to the access server, a specialized Axidian Privilege application is launched as a desktop shell with the following functions:

- User access rights check – permissions to access the desired target resource under the requested account.
- User authentication.
- Session video records and screenshots.
- Shadow copying of files transferred during the sessions.

The following client software is used to start new sessions in the target systems and applications on the access server:

- Microsoft RDP client (MSTSC) for Windows server connections.
- A browser for web application connections.
- PuTTY client for SSH and Telnet connections.
- Specialized client software for connections to various information systems via proprietary protocols (thick client).

RDP Proxy

RDP Proxy is an Axidian Privilege module used for connections to target resources via RDP.
RDP Proxy and the access server have similar functions:

- User access rights check.
- User authentication.
- Session video records and screenshots.
- Shadow copying of files transferred during the sessions.

Its key differences from the access server are as follows:

- It is based on free software.
- Docker serves as a deployment platform, which eliminates the need to use a server running Windows for deployment.

The user can open new sessions on target resources by using the RDP client to initiate the connection to RDP Proxy from their workstation. When users connect to the proxy, they will need to complete authentication. During this process, they may be prompted to provide a second authentication factor, and their access permissions will be checked. After this, an RDP session will be launched on the target resource.

SSH Proxy

SSH Proxy is the basic way to connect to Linux/Unix systems via Axidian Privilege. This method has the following advantages:

- You don't need to use Microsoft RDS.
- You can use any SSH client.
- The SSH client can run locally on the user workstation used for PAM connection.

SSH Proxy and the access server have similar functions:

- User access rights check.
- User authentication.
- Session text log (all SSH input/output is recorded).

With SSH Proxy, users can work with the same familiar SSH client to initiate connections from their workstation. The SSH Proxy address should be indicated as the connection server. All users trying to connect to SSH Proxy may be prompted to provide a second authentication factor, and then a new session will be launched on the target resource.

Filter for commands

In SSH sessions, the PAM administrator has the option to make a list of permitted and forbidden commands for specific target resources (the list of resources is stipulated by the scope of a relevant policy). Two modes are available for the command filter:

- Anything that is not forbidden is allowed. In this case, the administrator can specify the list of forbidden commands.
- Anything that is not allowed is forbidden. This is a more rigid filter where the administrator should expressly indicate the allowed commands and disable all other commands.

Regular expressions are used to describe the commands. You can set the following reactions in response to a forbidden command entry:

- Terminate the session.
- Abort the command.

SFTP and SCP

In addition to the SSH protocol, SSH Proxy also supports SFTP and SCP for connections to target resources. The procedure is similar to SSH connection, i.e., a user should indicate SSH Proxy address as the connection server. All users trying to connect to SSH Proxy may be prompted to provide a second authentication factor, and then a new session will be launched on the target resource.

For SFTP and SCP protocols, SSH Proxy creates a session text log that captures all file operations performed by the user.

It is possible to control the direction of data transfer via SCP/SFTP.

Port forwarding

You can use SSH proxy to forward ports from a target resource to a local host. This enables users to execute familiar scenarios and use their preferred tools to administer target resources.

PAM control server

The PAM control server is the central module of the Indeed PAM system responsible

for data exchange and smooth operation of other modules. The key needs addressed by the server are as follows:

- Centralized management of all system data (users, resources, credentials, permissions, policies, etc.).
- Encryption of critical data in the PAM database (privileged credentials, etc.).
- Completion of scheduled tasks (user account searches, password rotation, etc.).
- Provision of an API for integration with third-party systems.

Identity Provider (IDP)

The Identity Provider (IDP) enables two-factor user authentication for connections to all PAM modules. For authentication via AD or FreeIPA, the first factor is the user's domain password, and the second factor is a one-time password generated in the app installed on the user's smartphone or sent by email. For authentication via RADIUS, the factors are determined by the external multi-factor authentication system.

If one-time passwords are generated in the app installed on the smartphone, users will be prompted to register the OTP app upon their first login in the management console or user console. After successful registration, they are granted access to the system.

If OTPs are sent by email, the password will be sent to the user’s email address obtained by PAM from the user’s profile in the user directory.

Besides user login, IDP is also instrumental for authentication of applications that rely on the PAM server API.

Connectors

Connectors have multiple functions in privileged account management:

- Routine searches for new privileged accounts on the target resources. This is a protective measure against unscrupulous administrators that may create special accounts to bypass the PAM system.
- Routine checks of passwords and SSH keys to privileged accounts. This feature can help you make sure that all credentials in the PAM vault are up to date and malevolent administrators cannot bypass the PAM system by resetting the password.
- Routine password and SSH key change. Axidian Privilege can generate random complex passwords and SSH keys for managed privileged credentials, thereby protecting them from unauthorized access.
- Password reset after disclosure to the user. The PAM administrator may allow users to view their passwords to privileged accounts if they need to use such a password explicitly. In this case, Axidian Privilege will reset the password to a new random value after a certain period of time.

Axidian Privilege includes connectors for the following target systems:

- Active Directory

- Windows
- SSH connector for Linux/Unix connections in various distributions
- DBMS connector (MS SQL, Oracle, PostgreSQL, etc.)
- Cisco IOS
- Inspur BMC

Management console

The management console is a web application that serves as an interface for system customization and audits. Administrators can use the console to grant users access to credentials and resources, set up access policies, and view event logs and privileged session records. The console can also be utilized for real-time monitoring of active privileged sessions that can be terminated by the PAM administrator if needed. Users must complete two-factor authentication to gain access to the management console.

User console

The user console is made as a web application. The console features all the permissions granted to the user; they can run searches by address or resource name, connection protocol, or account name. After locating the desired resource for connection, the user should download an RDP file that contains the required parameters. This file can be saved and used again; you do not need to download a new file every time. For SSH resources, you can copy the connection string to clipboard and use it with any SSH client.

In the console, users can also view, set, or change privileged credentials for which they have permissions. Two-factor authentication is required for gaining access to the user console.

Users can independently group available resources into folders to reduce the workload of PAM administrators and customize their workspace.

Deployment model

Axidian Privilege includes multiple functional modules which may be installed on various servers. The selected deployment model depends on testing and operation scenarios.

The following deployment models are available:

- Simplified model. All Axidian Privilege functional modules are installed on one server. This option is recommended for testing and getting familiar with the solution.
- Basic model. Axidian Privilege functional modules are installed on different servers. This model allows segregating the functional modules that define the system's operation logic from the functional modules responsible for access. This option is recommended for industrial implementation and operation.
- Fail-safe model. Axidian Privilege functional modules are installed on different

servers, and each server is mirrored to ensure fail-safe operation. This option is recommended for industrial implementation and operation.

Below you will find an example of the basic deployment model and scenarios of access to protected resources for users and access to the Axidian Privilege control server for Axidian Privilege administrators.

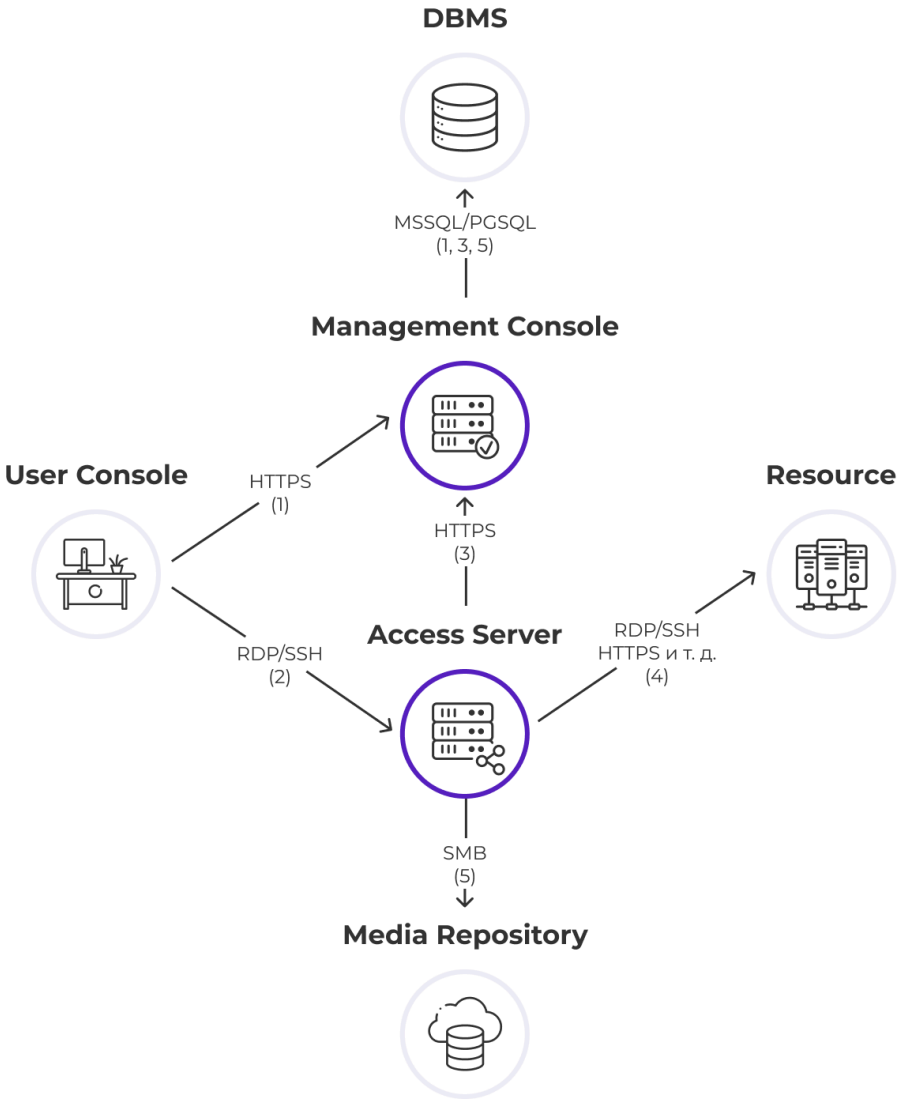

Figure 3. Basic deployment model.
Access to protected resources by a target user.

1. Connecting to the user console in a browser. Domain authentication and second factor registration/provision. Verification of user credentials in the IDP database. Obtaining the list of resources from the Core database. Obtaining an RDP file to connect to a resource.
2. Connecting to the access server using an RDP file or an SSH client selected by the user.
3. Domain authentication and provision of the second factor. User verification in IDP database. Verification of access permission in the Core database.

Extraction of the service account login and password from the DBMS to interact with the media repository. Extraction of the privileged account login and password from the DBMS to connect to the resource.

4. Connecting to the resource.
5. Saving video records and screenshots in the media repository. Saving the text log in the Core database.

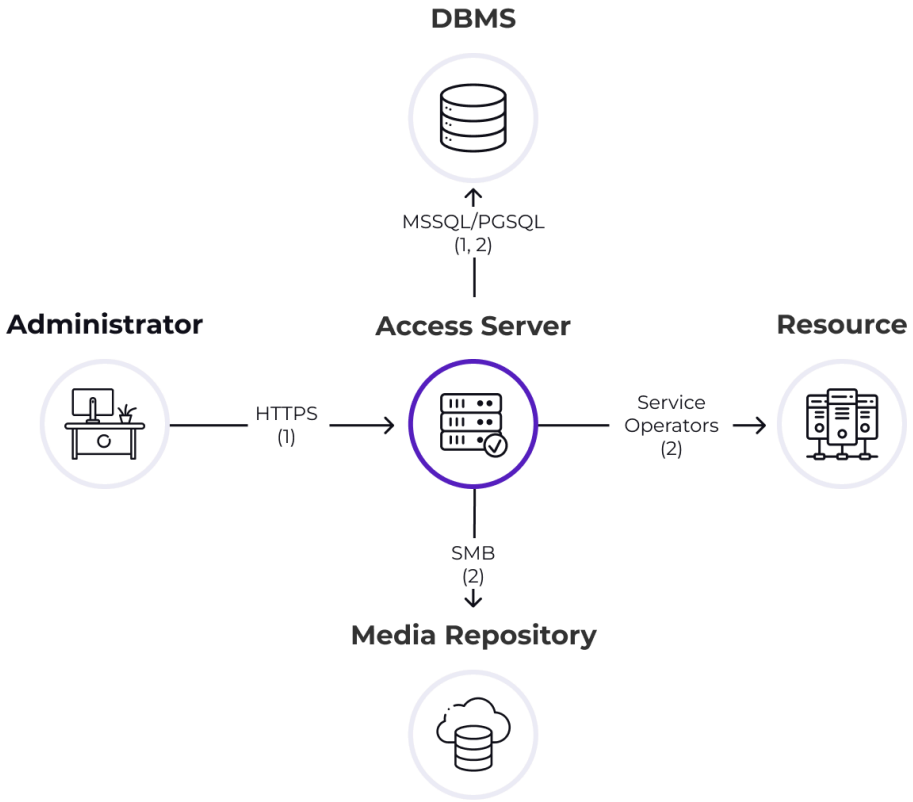

Figure 4. Basic deployment model.
Axidian Privilege administrator access.

1. Connecting the administrator to the management console in a browser. Domain authentication and second factor registration/provision. Verification of administrator credentials in IDP database.
2. Obtaining, adding, and editing of objects in the system. Performing service operations.

Supported deployment platforms

Indeed PAM can be installed on servers running both Windows and Linux. The product is supplied in distribution packages for Windows or as Docker images for Linux. When deploying the product in Docker on Linux, you can use automation tools to prepare the environment on nodes and deploy system modules.

Axidian Privilege key features

Access protocols	RDP SSH HTTP(s) TELNET SFTP SCP Any protocol via client publication
Supported types of managed credentials	Login + password SSH key
Privileged account search and password management	Windows Linux Active Directory DBMS (MS SQL, PostgreSQL, MySQL, Oracle, etc.) Cisco IOS Inspur BMC
Supported user directories	Active Directory FreeIPA
Two-factor user authentication technology	Password + TOTP (password generation algorithm) Password + OTP sent by email Smart card with a digital certificate[2] RADIUS
Supported session log types	Text log Video records Screenshots
Remote access technologies	Microsoft RDS SSH Proxy RDP Proxy
Supported deployment platforms	Windows Server 2012 R2 – 2022 Any Linux OS supported by Docker

[2] Only when Microsoft RDS is used.

About Axidian

Axidian is a global IT security vendor with a corporate center located in Dubai, UAE, and branches in Lithuania and Singapore.

Our core belief is that IT security should be accessible to every organization and considered as an investment not an expense. We deliver authentication and comprehensive access management, PAM, identity threat detection and response and PKI management solutions worldwide through the global partnership network. Our mission is to make resilient IT security possible for companies across the world.

Axidian offers:

- One-stop-shop for corporate identity security solutions (products that cover various scenarios, no need to look for different vendors, waste resources, support integration)
- Two licensing models to make privileged access management accessible and cost-effective for any type of enterprise.
    - Privileged Users (licenses by users and resources, licenses could be recalled, easy to calculate)
    - Privileged Sessions (licenses by number of simultaneous connections, no need to recall licenses, experience of work with PAM required)
- Quick and efficient assistance by local teams, availability of experts on-site, wide presence in over 30 countries through local partners

If you have any questions about our products or interested in more detailed information on those, please visit axidian.com.

Our contacts

axidian.com

sales-europe@axidian.com

sales-mena@axidian.com

sales-asia@axidian.com

www.linkedin.com/company/axidian